Ingentis org.manager for SAP SuccessFactors: Security Statement

Project:	IOM SF
Classification:	Public
Version:	1.1
As of:	11.07.2025

Ingentis Softwareentwicklung GmbH · Raudtener Str. 7 · 90475 Nuremberg / Germany · +49 (0) 911 98 97 59-0 · mail@ingentis.com · www.ingentis.com
Managing Directors: Joachim Rotzinger (CEO) · Tobias Weiß (COO)
VAT ID DE186953155 · Tax (Steuer) Nr.: 241/115/70031 · Amtsgericht Nuremberg · HRB: 14491

Contents

General

Ingentis org.manager for SAP SuccessFactors is an extension to SAP SuccessFactors first released in 2015. Benefiting from over 25 years of experience in the segment of organizational charts, the solution is designed for the swift creation of custom organizational charts for SAP SuccessFactors.

Ingentis org.manager for SAP SuccessFactors runs on SAP Business Technology Platform and is integrated in SAP SuccessFactors. The tool is certified by SAP as SAP SuccessFactors Extension build on SAP Business Technology Platform.

Certifications and Privacy

Ingentis has been TISAX-certified since November 2021. The org.manager product has also been independently audited and received a SOC 2 Type 2 report, and has been premium certified by SAP SE as an SAP Endorsed App. ISO 27001 and SOC 2 certifications cover the entire infrastructure, including SAP BTP and hyperscalers.

Ingentis strictly complies with the EU General Data Protection Regulation, with compliance and the necessary technical measures (TOMs) being regularly checked by an external data protection officer.

We maintain internal information security policies, including security incident response and business continuity plans, and we regularly review and update these.

Ingentis provides its employees with regular security and technology usage training according to TISAX. Our employees must sign a privacy agreement.

Our engineers adhere to best practices and industry-standard secure coding guidelines that align with the OWASP Top 10.

Both the TISAX and SOC 2 reports can be shared under an NDA.

Data Residency

Org.manager and all used SAP technologies are hosted on the SAP Business technology platform. New tenants will be onboarded in the nearest environment to the underlying SuccessFactors system of the customer. The following data centers and hyperscalers are used in the regions listed below:

Region	Hyperscaler	Location	SAP Regional Name	SAP Regional Identifier	Hyperscaler Regional Name
Europe	Microsoft Azure	Amsterdam (Netherlands)	Europe (Netherlands)	eu-20	West Europe
USA	Microsoft Azure	Quincy (Washington)	US West (WA)	us-20	West US 2
Canada	Amazon Web Services	Montreal	Canada (Montreal)	ca-10	ca-central-1
Australia	Amazon Web Services	Sydney	Australia (Sydney)	ap-10	ap-southeast-2
Kingdom of Saudi Arabia	Google Cloud Plattform	Dammam	KSA (Dammam)	sa-31	me-central2

Org.manager only runs on SAP Business Technology Platform data centers. SAP ensures that the same or equivalent certificates are valid at every data center where cloud solutions are run:

- C5
- ISO/IEC 22301

- ISO/IEC 27001
- ISO/IEC 27017
- ISO/IEC 27018
- SOC 1 Type II
- SOC 2 Type II

For more detailed information have a look at the official compliance documentation of the data center in use.

Authentication/User Security and Management

All users are authenticated to the application via the SuccessFactors system or an alternative Identity Provider (IdP) using the SAML 2 protocol. User creation, changes to users and user deactivation, as well as the definition and administration of roles and rights, are thus carried out via the SuccessFactors system or IdP.

Org.Manager is secured via SSO and requests roles from the SuccessFactors system. This means that access to the application is only possible after authentication against the SF system (or IdP) and that no data can be viewed or actions performed without the correct role. The SSO configuration is stored in a tenant-specific extension account.

When accessing the org.manager configuration front end, users are automatically redirected to the underlying IdP. Once the user has been correctly authenticated, their roles are requested by the SuccessFactors system to determine their final permissions.

Once authenticated and authorized, the user and their permissions are identified via a session. Sessions have an idle timeout of 30 minutes and last for a maximum of 12 hours. After this time, the user must authenticate again. When a user is assigned new roles, they must log out and log back in again for the changes to take effect.

Attention: A technical user account is required for the system to work properly and it is recommended that a configuration user is also set up. You can find more information about these two types of user in the Deployment section.

Encryption

Data Encryption

To protect data saved to disk from unauthorized access at operating system level, the SAP HANA Cloud, SAP HANA database uses native SAP HANA data encryption in the persistence layer. Data volume encryption protects the data area on disk, while redo log encryption protects the log area on disk. All pages that reside in the data area on disk are encrypted using the AES-256-CTR algorithm. Log entries are also encrypted using the AES-256-CTR algorithm before they are written to disk.

Org.manager can use other data sources besides SuccessFactors. This data is stored in the same HANA Database as the data from the SF Data Sources and encrypted in the same way.

The connections within the SAP BTP are secured via TLS 1.3 and encrypted with the TLS_AES_256_GCM_SHA384 and TLS_AES_128_GCM_SHA256 cipher suites.

Network Encryption

All connections to the application are secured via TLS 1.2.

Segregation

A separate scheme, user and password is generated for every tenant, so that every tenant has its separate JDBC connection to the database. In addition, a main connection exists with a separate user and scheme, so non tenant specific information can be stored.

Monitoring

To be able to maintain technical availability, the systems of org.manager for SAP SuccessFactors are monitored automatically by SAP as platform provider.

Additionally, to the technical availability, Ingentis is monitoring the application for the following:

- CPU usage

- Memory usage
- Disk usage
- Network transfer rate
- Database availability
- Database memory/cpu usage.
- Requests per minute to the application
- Users per minute
- Errors per minute
- Feature usage

Availability of the application can be checked at status.ingentis.com.

Logging

Application logs are securely stored within SAP BTP for 30 days. When the logs are generated, the internal system clock of SAP BTP is used. The logs are protected against manual modifications even by the administrator.

The following application events are being logged:

- Application errors
- Application starts/shutdowns
- HTTP access log

Configuration logs are securely stored till termination of the contract. When the logs are generated, the internal system clock of SAP BTP is used.

The following configuration events are being logged:

- Configuration changes
- Metadata refreshes
- Configuration replaced by another configuration
- License file changes
- Configuration resets
- Data in use resets

- Secret created/deleted (for SFTP)

All login attempts are redirected to the customer's SuccessFactors system and only valid attempts are processed by the application. The authentication is handled by customer's SF system and thereby the access logs are in the responsibility of the customer. Attention: System logs of the SAP BTP are not handled by Ingentis.

Security Tests

As part of their security standards, SAP has penetration testing performed by internal and external ethical hackers. However, the SAP penetration test report cannot be provided to customers, as it contains sensitive information.

Ingentis has penetration testing performed annually by an external service provider. If an NDA is in place, an excerpt of this test can be shared with a customer.

Backup and Disaster Recovery

A full backup of all SAP HANA Cloud instances is taken automatically once per day and every 15 minutes an incremental.

The recovery point objective (RPO) is 15 minutes. Backups are stored encrypted in an object store independent of a specific availability zone. The backup retention period is 14 days.

The recovery time objective (RTO) is 24 hours. Disaster recovery plans are reviewed and tested annually.